

FORÇAS ARMADAS
PORTUGUESAS

Cyber Defence

A Capability Development Contribution

Capt Helder Fialho de Jesus | Academia Militar | 19 Abril 2018
Chief of Cyberdefence Centre

Jaap de Hoop Scheffer



11 NATO SECGEN
(2004-2009)

We will also need to have a serious debate about the balance between land, air and naval forces. During my time as Secretary General I have seen the naval dimension rapidly grow in importance as we focus on piracy, the High North, the protection of maritime energy transportation networks, and the prevention of clandestine transfers of missile technology and weapons of mass destruction. NATO at sea in the 21st century could be just as important as NATO on land. This balance has to be better factored in to our planning and capability development. We also need to look at our level of ambition. Is it still the right one?

Ref: https://www.nato.int/cps/en/natolive/opinions_56153.htm

Anders Fogh Rasmussen



12 NATO SECGEN
(2009-2014)

So my question to you is: What's going to make future capability development qualitatively different, and in terms of time, different from NATO's past sluggish performance? Is it going to be mandatory NATO technical standards? Will it be the use of a new security label to promote standardized equipment? What will it be? Thank you.

Ref: https://www.nato.int/cps/en/natolive/opinions_85692.htm

Jens Stoltenberg



13 NATO SECGEN
(2014- . . .)

NATO's modern defence posture is based on an effective combination of cutting-edge weapons systems and platforms and forces trained to work together seamlessly. As important as it is that Allies invest in defence, it is also critical that those funds are invested in the right capabilities. NATO plays an important role in assessing what capabilities the Alliance needs, setting targets for national or collective development of capabilities, and facilitating national, multinational and collective capability development and innovation.

Ref: https://www.nato.int/cps/en/natohq/opinions_142149.htm

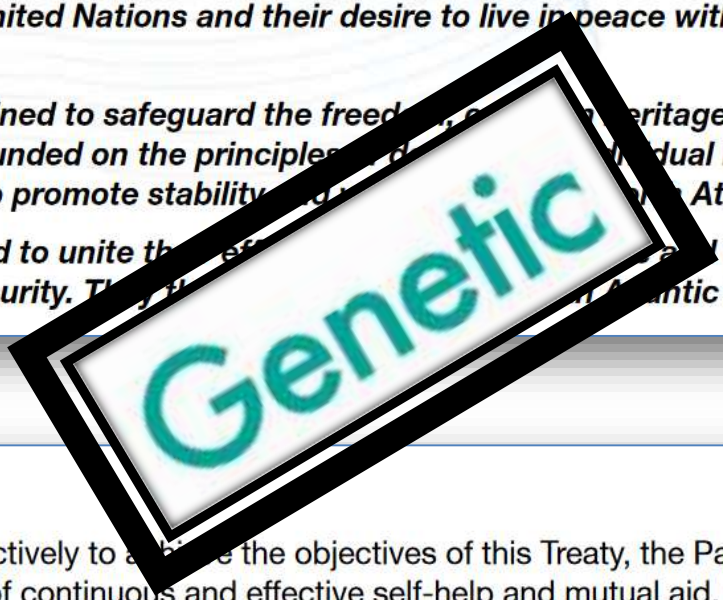
The North Atlantic Treaty (1949)

Washington D.C. - 4 April 1949

The Parties to this Treaty reaffirm their faith in the purposes and principles of the Charter of the United Nations and their desire to live in peace with all peoples and all governments.

They are determined to safeguard the freed[illegible] heritage and civilisation of their peoples, founded on the principles [illegible] dual liberty and the rule of law. They seek to promote stabilit[illegible] Atlantic area.

They are resolved to unite th[illegible] for the preservation of peace and security. T[illegible] ntic Treaty:



Article 3

In order more effectively to a[illegible]e the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.

2016 Cybersecurity Skills Gap



Too Many Threats

$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) **RECORDS STOLEN IN 2014**[1]

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO **NATIONAL SECURITY AND ECONOMIC STABILITY**[2]

MORE THAN **1 IN 4** ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[3]

$150 MILLION: AVERAGE COST OF A **DATA BREACH BY 2020**[4]

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S **INTERNET OF THINGS (IOT) DEVICES**[5]

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING **HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM**[6]

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY **PROFESSIONALS BY 2019**[7]

3X **RATE OF CYBERSECURITY JOB GROWTH** VS. IT JOBS OVERALL, 2010-14[8]

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR **OPEN SECURITY JOBS ARE QUALIFIED**[9]

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS **6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES**[10]

77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. **FOR MEN, IT IS 67%.**[11]

89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO **HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.**[12**]

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

SOURCES: 1. *2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015.* **2.** *ISACA 2015 APT Study, October 2015.* **3.** *ISACA 2015 APT Study.* **4.** *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015.* **5.** *SACA 2015 IT Risk/Reward Barometer-Member Study, September 2015.* **6.** *ISACA 2015 IT Risk/Reward Barometer-Member Study.* **7.** *UK House of Lords Digital Skills Committee.* **8.** *Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2015.* **9.** *State of Cybersecurity: Implications for 2015, ISACA and RSA Conference, April 2015.* **10.** *State of Cybersecurity: Implications for 2015.* **11.** *Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2015.* **12.** *2015 ISACA Risk/Reward Barometer-Consumer Study, September 2015.*

** "Employees" refers to data security professionals at organizations that potentially have access to survey respondent's personal information.

CSX CYBERSECURITY NEXUS

ISACA *Trust in, and value from, information systems*

https://cybersecurity.isaca.org January 2016





Conclusions (2017)

The past two years have seen a clear demonstration of the potentially disruptive effects of cyberattacks on all critical sectors. Loose coordination and soft policies are a first step but will clearly be insufficient to face new, complex and cross-border threats. Cybersecurity needs to become a political priority. **Anticipating and planning for the worst should drive the next steps at European level**. Robust policies on cybersecurity and the development of European capabilities, underpinned by significant EU funding, should form the basis of a European cyber shield to defend EU institutions, Member States, businesses and citizens.


Cyber Security Week
powered by The Hague Security Delta
25 - 29 September 2017
The Hague, The Netherlands
Toolkit | Pressroom
About
Programme
Matchmaking
Automation
Multinational Cyber Defence
Development: NATO Comm
Information Agency
nised by
NCI AGENCY
Incident resp
and complexity of cyberattacks is
on the rise. De
unable to respond to security events
effectively. Manu
ocesses are no longer enough; mature
incident response
the need for automation. At the request of
several nations, the
mmunications and Information Agency is performing
an assessment of the
dent response orchestration market. This session will
provide an overview of the market, describe some of the major issues to consider
when assessing an incident response orchestration solution, discuss some of the
limits of automation, and explore the various directions the market is following.

How is NATO Meeting the Challenge of Cyberspace?

By Jamie Shea

Historians of international relations are familiar with the hinge-year concept when trends that previously had been largely subterranean suddenly crystallize into a clear and immediate danger, forcing policymakers to wake
smashed any complacency abou
tacks. As fast as we have tried to
2016 witnessed the first major at
was hacked through video surve
and increasing evidence of collu

Yet it is not the much discusse
that has dominated the debate. It
and manipulation. From being a
evolved into a potent instrument
been the victim of an unprecede
2,000 orchestrated cyberattacks
election voting system, train and
elimination of tax and financial
ware attack similar to the previo
countries, it soon became clear t
was not financial gain but rather
were also affected by NotPetya,
NotPetya was a state-driven effo
as a laboratory or proving ground to test a range of cyber weapons and assess their impact, with widespread collateral damage elsewhere accepted as a consequence of doing business; or even as a way to cover tracks.[2]

Given the difficulty of technical attribution and the inability of governments to deter or retaliate against cyberattacks in a manner that demands the attacker's attention but avoids unwanted escalation, NATO has

Dr. Jamie Shea is Deputy Assistant Secretary General for Emerging Security Challenges at NATO. The views expressed are entirely those of the author and should not be construed as an official position of NATO.



Whereas we have a good idea how to deter a nuclear or conventional attack, to deal with crises in the traditional domains, to employ arms control or confidence-building arrangements, we still do not have a good idea of how to deter or respond to major cyberattacks, even when they are clearly designed to undermine our governments or our political processes.

Capabilities – National Contribution







Proj 6.5 - Cyber Threats and Incident Response Information Sharing Platform

A Look at Four Security 2040 Projects

A series of RAND research projects is looking to the mid-future [illegible] the forces that will shape our path from here to there. The effort, [illegible] RAND as Security 2040, has one overarching goal: "The world is changing [illegible] said Andrew Lohn, an associate engineer at RAND and one of the lead researchers on the artificial-intelligence question. "We want to just be ahead of the curve."

Millennials



Photo by Yuri_Arcus/Getty Images

3-D Printing

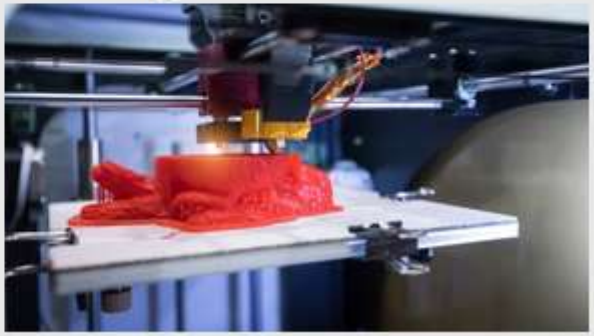


Photo by kynny/Getty Images

Artificial Intelligence



Photo by Ingo Wagner/Picture-Alliance/DPA/AP Images

Speed



Photo by Nicki Kohl/Telegraph Herald via AP Images



GLOBSEC

Future War NATO?

From Hybrid War
to Hyper War
via Cyber War

GLOBSEC
NATO
Adaptation
Initiative
Supporting paper

Future War NATO?

From Hybrid War to Hyper War via Cyber War

Supporting Paper of the GLOBSEC NATO Adaptation Initiative

By General (Ret.d) John Allen, General (Ret.d) Philip M. Breedlove,
Professor Dr Julian Lindley-French, & Admiral (Ret.d) George Zambellas



GLOBSEC

Future War NATO?

From Hybrid War
to Hyper War
via Cyber War

GLOBSEC
NATO
Adaptation
Initiative
Supporting paper

Future War NATO?

From Hybrid War to Hyper War via Cyber War

Supporting Paper of the GLOBSEC NATO Adaptation Initiative

By General (Ret.d) John Allen, General (Ret.d) Philip M. Breedlove,
Professor Dr Julian Lindley-French, & Admiral (Ret.d) George Zambellas

How NATO wants to use artificial intelligence in decision making

Nyshka Chandran | @nyshkac

Published 3:26 AM ET Sun, 4 June 2017 | Updated 12:04 AM ET Fri, 10 Nov 2017

CNBC



The North Atlantic Treaty Organization (NATO) believes in incorporating artificial intelligence in its decision-making process, a senior official told CNBC.

The 68 year-old military alliance is committed to exploring technological advancements, with effective mobilization of data and human capital among its key areas of focus, said General Denis Mercier, NATO's Supreme Allied Commander Transformation.

Speaking on the sidelines of this year's Shangri-La Dialogue, an annual gathering of defense ministers, Mercier said NATO "needs to develop a better big data approach, cloud-like architectures and make an extensive use of AI."

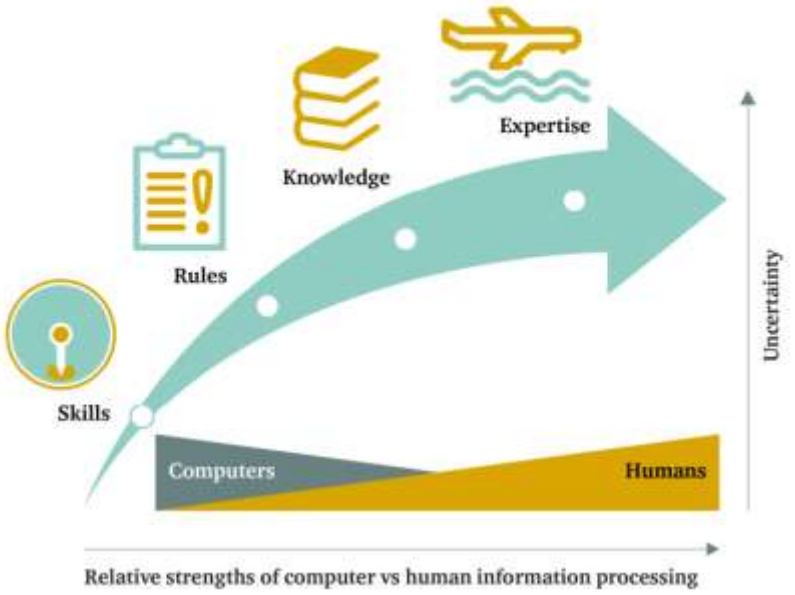
Research Paper

M. L. Cummings
International Security Department and US and the Americas Programme
January 2017

Artificial Intelligence and the Future of Warfare

CHATHAM HOUSE
The Royal Institute of International Affairs

Figure 2: The relationship between uncertainty and skill, rule, knowledge and exper reasoning



Capabilities

D O **T** M L P F I

Doctrine · Organization · **Training** · Material · Leadership · Personnel · Facilities · Interoperability

Collective Training and Exercises

NATO









EU



Ibero American



National



CyberDEx

CNCS
Centro Nacional de Cibersegurança
PORTUGAL



EXÉRCITO

2018 – 1st National Cyber Defence Exercise

Services

Analisys



Forens



Vulnerabilities



Network traffic



Penetration Testing



Event Correlation
(Monitorization & Analysis)



Malware
(reverse engineering)

Artificial Intelligence

"The Integrated Digital System" to CNO

Cyber CyCOP
(Common Operational Picture)

CNO - Computer Network Opertions

Cyber Academia and Innovation Hub
(Approved)

Stakeholders

- **Capability Building Requirements and Needs;**
- **CS & CD Education, Training and Exercises** (National, NATO, EU, …)

Industry

- **Innovation;**
- **Cyber R&D Projects** (National and International)

Universities

- **CS & CD Masters' Program;**
- **Cyber R&D Projects** (National and International)

NCI Academy (Oeiras)



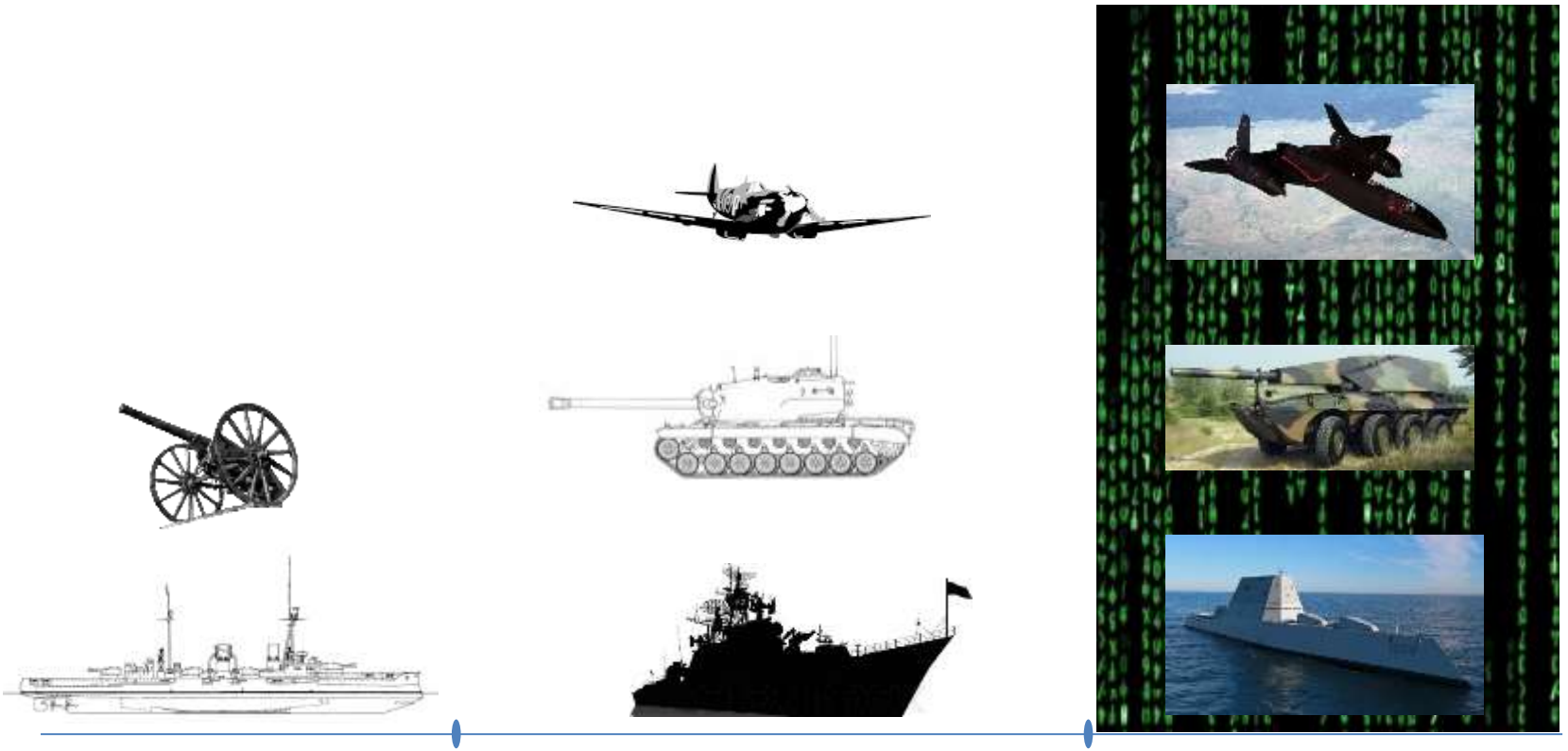




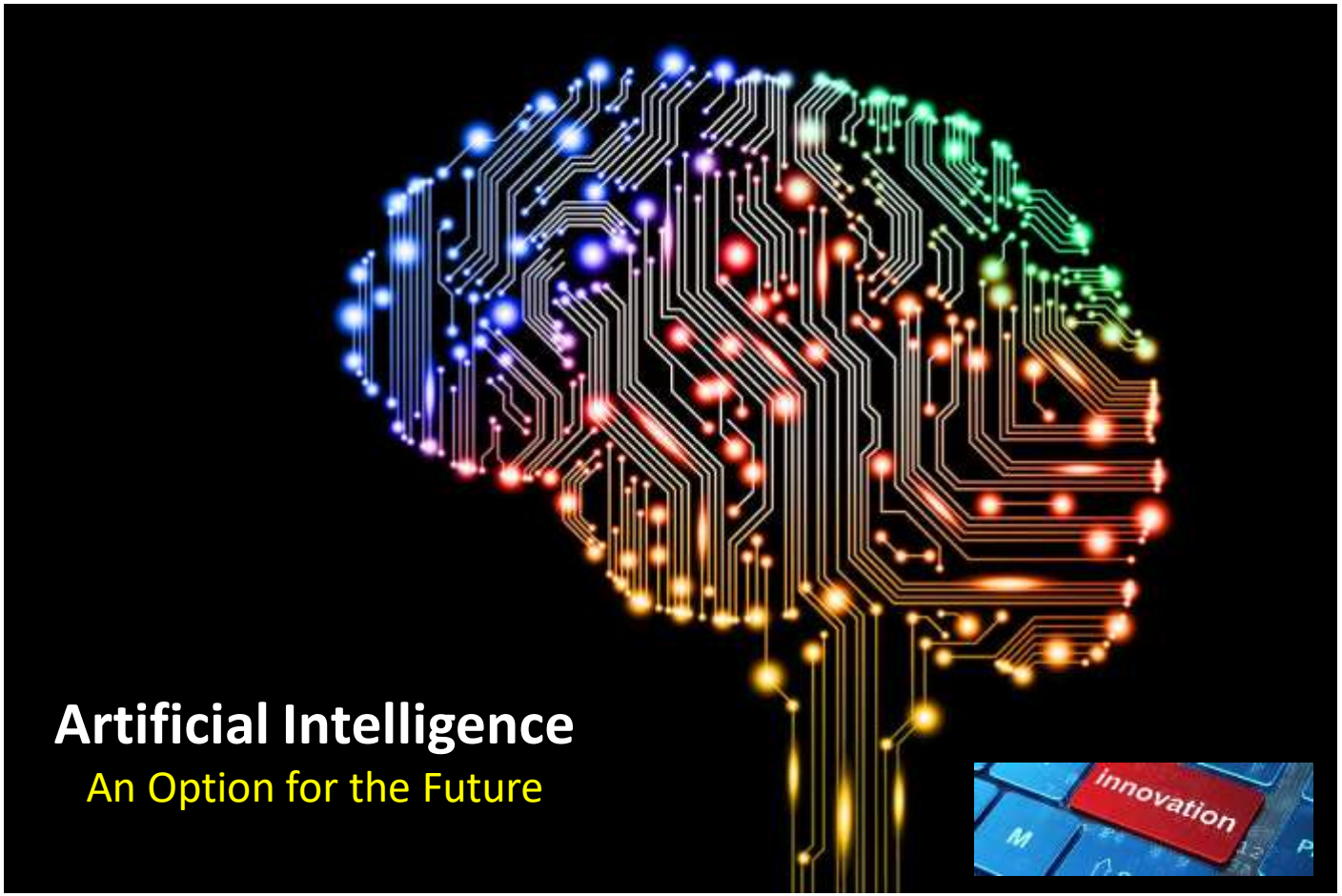
Stephen Hawking At Web Summit: Will Artificial Intelligence Help Us, Or Destroy Us?

INTELLIGENT MACHINES / NOV 08, 2017 / EMMA / 0 COMMENT

Evolution



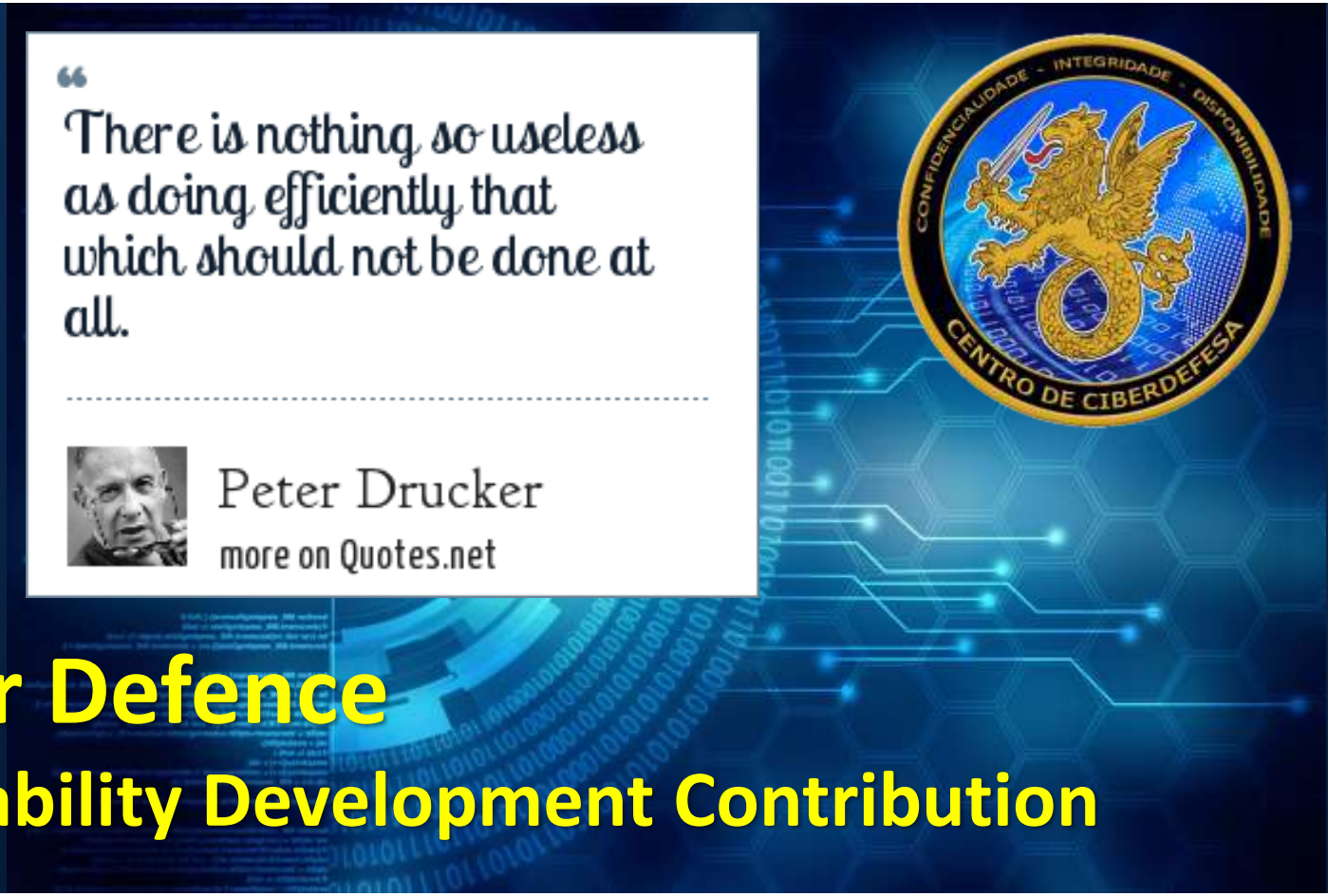
19th Century	20th Century	21th Century
2 Dimentions	3 Dimentions	4 Dimentions



Cyber Defence Capability Development – Enhancing Capability Building

EMGFA

CD SDP
CYBER DEFENCE
SMART DEFENCE PROJECTS



Cyber Defence
A Capability Development Contribution

Helder Fialho de Jesus
PRT Navy Captain – Chief of the Ciber Defence Centre (CCD)

Academia Militar, 19Apr2018